(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2000－341632
（P2000－341632A）
(43)公開日　平成12年12月８日(2000.12.8)

(51)Int.Cl.⁷	識別記号	ＦＩ		テーマコード（参考）
Ｈ０４Ｎ　5/91		Ｈ０４Ｎ　5/91	Ｐ	５Ｂ０１７
Ｇ０６Ｆ　12/14	３２０	Ｇ０６Ｆ　12/14	３２０Ｅ	５Ｃ０５３
Ｇ０９Ｃ　1/00	６４０	Ｇ０９Ｃ　1/00	６４０Ｄ	５Ｃ０７８
			６４０Ａ	５Ｊ１０４
5/00		5/00		９Ａ００１

審査請求　有　請求項の数18　ＯＬ　（全 14 頁）　最終頁に続く

(21)出願番号　特願平11－146959

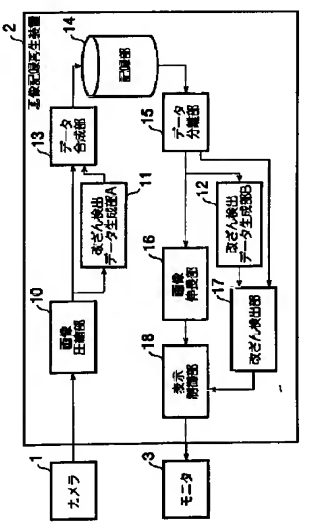
(22)出願日　平成11年５月26日(1999.5.26)

(71)出願人　000005821
松下電器産業株式会社
大阪府門真市大字門真1006番地
(72)発明者　青木　芳人
神奈川県横浜市港北区綱島東四丁目３番１号　松下通信工業株式会社内
(74)代理人　100082692
弁理士　蔵合　正博

最終頁に続く

(54)【発明の名称】　画像記録再生装置と画像再生装置と不正利用防止方法

(57)【要約】
【課題】　画像をデジタル信号で記録再生する装置において、デジタル画像の改ざんおよび第三者からの不正アクセスを防止することを目的とする。
【解決手段】　画像圧縮部10で圧縮されたデジタルデータから改ざん検出用データを改ざん検出部11で生成する。改ざん検出データは、デジタル画像データ形式の空き領域へ埋め込み、記録部14に蓄積される。また、記録部14から再生する時はデータ分離部15で改ざん検出データを抜き出すと共に、改ざん検出データ生成部12で求めたデータとの比較を改ざん検出部17で行い、改ざんされていない場合のみ、圧縮されたデジタルデータを画像伸長部16で伸長し、表示制御部18を通して画像が再生される。改ざんが検出された場合には、画像は表示されない。



【特許請求の範囲】

【請求項１】　画像情報を取り込みデジタル圧縮処理する画像圧縮部と、前記画像圧縮部で処理された圧縮画像データに対して改ざん検出用データを生成する改ざん検出データ生成部と、前記圧縮画像データと改ざん検出データを１組のデータに結合させるデータ合成部と、前記結合データを記録する記録部と、前記記録部に記録された圧縮画像データを再生する際に前記圧縮画像データと改ざん検出データとを分離するデータ分離部と、前記分離された圧縮画像データに対して前記改ざん検出データ生成部と同一のデータ生成を行う改ざん検出データ生成部と、前記改ざん検出データ同士を比較する改ざん検出部と、前記圧縮画像データを伸長する画像伸長部と、前記伸長された画像データのモニタ画面への表示を制御する表示制御部とを備えた画像記録再生装置。

【請求項２】　前記改ざん検出データ生成部で生成される改ざん検出データが、圧縮画像データ全体あるいは一部に対するチェックサムあるいはパリティあるいはＣＲＣ（Cyclic Redundancy Check）であることを特徴とする請求項１記載の画像記録再生装置。

【請求項３】　前記記録部に記録された前記圧縮画像データと前記改ざん検出データを１組として可換記録媒体へ複写可能な外部記録装置を備えた請求項１記載の画像記録再生装置。

【請求項４】　請求項３記載の画像記録再生装置により前記圧縮画像データと前記改ざん検出データとを複写された前記可換記録媒体を再生できる外部記録再生装置と、前記再生された前記圧縮画像データと前記改ざん検出データとを分離するデータ分離と、前記分離された圧縮画像データに対して前記改ざん検出データ生成部と同方式のデータ生成を行う改ざん検出データ生成部と、前記改ざん検出データ同士を比較する改ざん検出部と、前記圧縮画像データを伸長する画像伸長部と、前記伸長された画像データのモニタ画面への表示を制御する表示制御部とを備えた画像再生装置。

【請求項５】　前記外部記録装置がＤＶＤ－ＲＡＭドライブ、前記可換記録媒体がＤＶＤ－ＲＡＭディスクであることを特徴とする請求項４記載の画像再生装置。

【請求項６】　前記改ざん検出生成部と前記改ざん検出部と前記画像伸長部をソフトウェア処理で実行することを特徴とする特徴とする請求項４記載の画像再生装置。

【請求項７】　伸長された画像データを他の記録媒体へ複写する際に、画像データ内に画像記録時間および画像記録時条件を電子透かしで埋め込む電子透かし処理部を備えたことを特徴とする請求項４から６のいずれかに記載の画像再生装置。

【請求項８】　前記記録部へ蓄積されている特定の画像データを暗号化する暗号化部と、暗号化に用いる暗号鍵を管理する暗号鍵管理部と、暗号化されたデータを外部へ送信するネットワークインターフェースとを備えた請求項１記載の画像記録再生装置。

【請求項９】　請求項８記載の画像記録再生装置により暗号化されたデータを受信するネットワークインターフェースと、前記暗号化されたデータの復号化を行う復号化部と、受信したデータを記録する記録部と、暗号化に用いた暗号鍵を管理する暗号鍵管理部とを備えた請求項７記載の画像再生装置。

【請求項１０】　画像情報を取り込みデジタル圧縮処理する画像圧縮部と、前記画像圧縮部で処理された圧縮画像データを暗号化する暗号鍵を管理する暗号鍵記録部と、前記暗号鍵を用いて圧縮画像データを暗号化した暗号化データを生成する暗号化処理部と、前記暗号化データを記録する記録部と、前記記録部に記録された暗号化データを前記暗号鍵を用いて復号化し圧縮画像データを生成する復号化処理部と、前記圧縮画像データを伸長する画像伸長部と、前記伸長された画像データのモニタへの表示を制御する表示制御部と、前記暗号鍵を入力する鍵入力部とを備えた画像記録再生装置。

【請求項１１】　前記暗号化処理部は、共通鍵暗号方式を利用することを特徴とする請求項１０記載の画像記録再生装置。

【請求項１２】　前記暗号鍵記録部は、共通鍵暗号方式あるいは公開鍵暗号方式で暗号鍵を暗号化しておくことを特徴とする請求項１０または１１記載の画像記録再生装置。

【請求項１３】　前記暗号鍵を暗号化して暗号化暗号鍵を生成する暗号鍵暗号部と、前記暗号化暗号鍵と前記暗号化データを結合させるデータ合成部と、前記合成したデータを記録できる可換記録媒体と、前記可換記録媒体に記録する外部記録装置を付加した請求項１０から１２のいずれかに記載の画像記録再生装置。

【請求項１４】　請求項１３記載の画像記録再生装置により暗号化暗号鍵と暗号化データを記録された前記可換記録媒体を再生できる外部記録再生装置と、前記再生された暗号化暗号鍵と暗号化データを分離するデータ分離部と、前記分離された暗号化暗号鍵を復号化して管理する暗号鍵復号部と、前記可換記録媒体から前記暗号化データを再生する際に前記暗号化データを復号化し圧縮画像データを生成する復号化処理部と、前記圧縮画像データを伸長する画像伸長部と、前記伸長された画像データのモニタへの表示を制御する表示制御部と、前記暗号鍵を入力する鍵入力部とを備えた画像再生装置。

【請求項１５】　前記暗号鍵を暗号化して暗号化暗号鍵を生成する暗号鍵暗号部と、前記暗号化暗号鍵と前記暗号化データを外部へ送信するネットワークインターフェースとを備えた請求項１０記載の画像記録再生装置。

【請求項１６】　請求項１５記載の画像記録再生装置により暗号化暗号鍵と暗号化データを受信するネットワークインターフェースと、前記受信時の暗号鍵の管理を行う暗号鍵管理部と、伝送された暗号化データを記録でき

る記録部と、前記記録部から前記暗号化データを再生する際に前記暗号化データを復号化し圧縮画像データを生成する復号化処理部と、前記圧縮画像データを伸長する画像伸長部と、前記伸長された画像データのモニタへの表示を制御する表示制御部と、前記暗号鍵を入力する鍵入力部とを備えた画像再生装置。

【請求項１７】　画像データの記録時に圧縮データから改ざん検出データを生成し、画像データと改ざん検出データを組にして記録部へ記録しておき、再生時は、画像データから新たに生成する改ざん検出データと記録時に生成された改ざん検出データとの比較によって、改ざん検出を行う不正利用防止方法。

【請求項１８】　ファイル毎に管理された暗号鍵を保存し、その暗号鍵で暗号化処理を行った画像データを記録し、再生時には入力された暗号鍵で暗号データを復号化することにより、暗号鍵を知らない者による画像の閲覧を防止する不正利用防止方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、カメラで撮像された画像信号をデジタル信号で圧縮、蓄積、伸長、伝送する際にデータ暗号化を行う画像記録再生装置と画像再生装置と不正利用防止方法に関する。

【０００２】

【従来の技術】図13に従来のこの種の画像記録再生装置の構成例を示す。図13において、101はカメラ、102 は画像記録再生装置、103 はモニタである。画像記録再生装置102 において、104 はA/D 変換器、105 は画像圧縮エンコーダ、106 は記録部、107 は画像伸長デコーダ、108 はD/A 変換器、109 はパスワード処理部である。

【０００３】記録時の動作は以下の通りである。カメラ101 で撮像された画像信号は、画像記録再生装置102 へ取り込まれ、A/D 変換器104 でデジタル信号へ変換され、画像圧縮エンコーダ105 で帯域圧縮され情報量が減らされる。圧縮された情報は、記録部106 （ハードディスクドライブ、光ディスク、テープが多い）へ記録される。

【０００４】一方、再生時は、記録部106 から再生すべきデータを検索し、画像伸長デコーダ107 へ入力され、データ伸長することで原画像データへ戻される。このデータをD/A 変換器108 でアナログ信号へ戻し、モニタ103 に映像が映し出される。また、画像記録再生装置102 の操作や装置の設定変更を行う場合には、パスワード管理部が109 がパスワードの入力を促し、正しいパスワードの入力があったかどうかを判断し、正しい時に限り、本装置での記録再生動作を実行できるようにする。

【０００５】

【発明が解決しようとする課題】しかしながら、上記従来の画像記録再生装置においては、圧縮された画像データは汎用の画像圧縮方式（JPEG等）を用いる例が多く、標準化されているJPEGではデータ形式が一般に公開されているため、圧縮データをそのままハードディスク等の記録装置へ記録している場合には、特定のデータ列の検索により圧縮データが記録されている位置の特定が比較的簡単に行うことができる。つまり、第三者が、記録装置本体からハードディスクを取り外して、画像データの記録位置を特定できさえすれば、パソコンの汎用グラフィックスソフトで画像を表示させることは簡単である。同様に、画像の一部を変更し、再度ハードディスクの同一位置に記録し直すことで改ざんも可能である。特に、監視機器市場で急速に進む画像のデジタル化では、上述のデータ改ざんの危険性が指摘されており、記録した画像の証拠性の有無にも関わる重大な課題となっている。

【０００６】本発明は、上記従来の課題を解決するもので、デジタルで記録される画像データの盗み見や改ざんを防止する機能を備えた画像記録再生装置および画像再生装置、および不正利用防止方法を提供することを目的とする。

【０００７】

【課題を解決するための手段】上記目的を達成するために本発明は、画像データの記録時に圧縮データから改ざん検出データを生成し、画像データと改ざん検出データを組にして記録部へ記録しておき、再生時は、画像データから新たに生成する改ざん検出データと記録時に生成された改ざん検出データとの比較によって、改ざん検出を行うようにしたものである。また本発明は、ファイル毎に管理された暗号鍵を保存し、その暗号鍵で暗号化処理を行った画像データを記録し、再生時には入力された暗号鍵で暗号データを復号化することにより、暗号鍵を知らない者による画像の閲覧を防止するようにしたものである。以上により、デジタルで記録される画像データの盗み見や改ざんを防止する機能を備えた画像記録再生装置および画像再生装置、および不正利用防止方法を得ることができる。

【０００８】

【発明の実施の形態】本発明の請求項１に記載の発明は、画像情報を取り込みデジタル圧縮処理する画像圧縮部と、前記画像圧縮部で処理された圧縮画像データに対して改ざん検出用データを生成する改ざん検出データ生成部と、前記圧縮画像データと改ざん検出データを１組のデータに結合させるデータ合成部と、前記結合データを記録する記録部と、前記記録部に記録された圧縮画像データを再生する際に前記圧縮画像データと改ざん検出データとを分離するデータ分離部と、前記分離された圧縮画像データに対して前記改ざん検出データ生成部と同一のデータ生成を行う改ざん検出データ生成部と、前記改ざん検出データ同士を比較する改ざん検出部と、前記圧縮画像データを伸長する画像伸長部と、前記伸長された画像データのモニタ画面への表示を制御する表示制御部とを備えた画像記録再生装置であり、従来の画像記録

のデータ形式の変更を伴わず、簡単に改ざん検出を行うことができるという作用を有する。

【０００９】また、請求項２に記載の発明は、前記改ざん検出データ生成部で生成される改ざん検出データが、圧縮画像データ全体あるいは一部に対するチェックサムあるいはパリティあるいはＣＲＣ（Cyclic Redundancy Check）であることを特徴とする請求項１記載の画像記録再生装置であり、改ざん検出データを簡単な計算方法で高速に生成することができるという作用を有する。

【００１０】また、請求項３に記載の発明は、前記記録部に記録された前記圧縮画像データと前記改ざん検出データを１組として可換記録媒体へ複写可能な外部記録装置を備えた請求項１記載の画像記録再生装置であり、可換記録媒体を用いて画像記録再生装置から外部へ画像データの取り出しが行えるという作用を有する。

【００１１】また、請求項４に記載の発明は、請求項３記載の画像記録再生装置により前記圧縮画像データと前記改ざん検出データとを複写された前記可換記録媒体を再生できる外部記録再生装置と、前記再生された前記圧縮画像データと前記改ざん検出データとを分離するデータ分離と、前記分離された圧縮画像データに対して前記改ざん検出データ生成部と同方式のデータ生成を行う改ざん検出データ生成部と、前記改ざん検出データ同士を比較する改ざん検出部と、前記圧縮画像データを伸長する画像伸長部と、前記伸長された画像データのモニタ画面への表示を制御する表示制御部とを備えた画像再生装置であり、可換記録媒体を用いて画像記録再生装置から外部へ取り出した画像データに対しても改ざん検出機能を継承し、より広範囲での改ざん防止を行えるという作用を有する。

【００１２】また、請求項５に記載の発明は、前記外部記録装置がＤＶＤ－ＲＡＭドライブ、前記可換記録媒体がＤＶＤ－ＲＡＭディスクであることを特徴とする請求項４記載の画像再生装置であり、大容量、低価格であり、再生時のデータ検索性を向上できるという作用を有する。

【００１３】また、請求項６に記載の発明は、前記改ざん検出生成部と前記改ざん検出部と前記画像伸長部をソフトウェア処理で実行することを特徴とする特徴とする請求項４記載の画像再生装置であり、専用のハードウエアや拡張ボードを用いないため低価格で実現できるという作用を有する。

【００１４】また、請求項７に記載の発明は、伸長された画像データを他の記録媒体へ複写する際に、画像データ内に画像記録時間および画像記録時条件を電子透かしで埋め込む電子透かし処理部を備えたことを特徴とする請求項４から６のいずれかに記載の画像再生装置であり、切り出した画像がさらに複製され続けても、改ざん検出と付加情報参照が行えるという作用を有する。

【００１５】また、請求項８に記載の発明は、前記記録部へ蓄積されている特定の画像データを暗号化する暗号化部と、暗号化に用いる暗号鍵を管理する暗号鍵管理部と、暗号化されたデータを外部へ送信するネットワークインターフェースとを備えた請求項１記載の画像記録再生装置であり、電子通信を通じて外部へ改ざん防止を施した画像データを送出が行えるという作用を有する。

【００１６】また、請求項９に記載の発明は、請求項８記載の画像記録再生装置により暗号化されたデータを受信するネットワークインターフェースと、前記暗号化されたデータの復号化を行う復号化部と、受信したデータを記録する記録部と、暗号化に用いた暗号鍵を管理する暗号鍵管理部とを備えた請求項７記載の画像再生装置であり、電子通信を通じた外部からの再生制御においても改ざん検出が行えるという作用を有する。

【００１７】また、請求項１０に記載の発明は、画像情報を取り込みデジタル圧縮処理する画像圧縮部と、前記画像圧縮部で処理された圧縮画像データを暗号化する暗号鍵を管理する暗号鍵記録部と、前記暗号鍵を用いて圧縮画像データを暗号化した暗号化データを生成する暗号化処理部と、前記暗号化データを記録する記録部と、前記記録部に記録された暗号化データを前記暗号鍵を用いて復号化し圧縮画像データを生成する復号化処理部と、前記圧縮画像データを伸長する画像伸長部と、前記伸長された画像データのモニタへの表示を制御する表示制御部と、前記暗号鍵を入力する鍵入力部とを備えた画像記録再生装置であり、画像記録再生装置内での画像データの暗号化により、画像データの改ざんや不正再生を防止することができるという作用を有する。

【００１８】また、請求項１１に記載の発明は、前記暗号化部は、共通鍵暗号方式を利用することを特徴とする請求項１０記載の画像記録再生装置であり、データの暗号化を高速に行うことができるという作用を有する。

【００１９】また、請求項１２に記載の発明は、前記暗号鍵暗号化部は、共通鍵暗号方式あるいは公開鍵暗号方式を利用することを特徴とする請求項１０または１１記載の画像記録再生装置であり、暗号鍵の伝送中の盗聴を防止できるという作用を有する。

【００２０】また、請求項１３に記載の発明は、前記暗号鍵を暗号化して暗号化暗号鍵を生成する暗号鍵暗号部と、前記暗号化暗号鍵と前記暗号化データを結合させるデータ合成部と、前記合成したデータを記録できる可換記録媒体と、前記可換記録媒体に記録する外部記録装置を付加した請求項１０から１２のいずれかに記載の画像記録再生装置であり、可換記録媒体に記録するデータを暗号化することで、第三者の無断再生を禁止する機能をより強化できるという作用を有する。

【００２１】また、請求項１４に記載の発明は、請求項１３記載の画像記録再生装置により暗号化暗号鍵と暗号化データを記録された前記可換記録媒体を再生できる外部記録再生装置と、前記再生された暗号化暗号鍵と暗号

化データを分離するデータ分離部と、前記分離された暗号化暗号鍵を復号化して管理する暗号鍵復号部と、前記可換記録媒体から前記暗号化データを再生する際に前記暗号化データを復号化し圧縮画像データを生成する復号化処理部と、前記圧縮画像データを伸長する画像伸長部と、前記伸長された画像データのモニタへの表示を制御する表示制御部と、前記暗号鍵を入力する鍵入力部とを備えた画像再生装置であり、可換記録媒体に記録された暗号化データを復号化することで、第三者の無断再生を禁止する機能をより強化できるという作用を有する。

【００２２】また、請求項１５に記載の発明は、前記暗号鍵を暗号化して暗号化暗号鍵を生成する暗号鍵暗号部と、前記暗号化暗号鍵と前記暗号化データを外部へ送信するネットワークインターフェースとを備えた請求項１０記載の画像記録再生装置であり、電子通信により遠隔地に対し暗号化データを送出することができ、第三者からの不正アクセスに対してもデータの安全性が確保できるという作用を有する。

【００２３】また、請求項１６に記載の発明は、請求項１５記載の画像記録再生装置により暗号化暗号鍵と暗号化データを受信するネットワークインターフェースと、前記受信時の暗号鍵の管理を行う暗号鍵管理部と、伝送された暗号化データを記録できる記録部と、前記記録部から前記暗号化データを再生する際に前記暗号化データを復号化し圧縮画像データを生成する復号化処理部と、前記圧縮画像データを伸長する画像伸長部と、前記伸長された画像データのモニタへの表示を制御する表示制御部と、前記暗号鍵を入力する鍵入力部とを備えた画像再生装置であり、電子通信による遠隔地からの再生要求に対して転送データを再度暗号がすることが不要となるとともに、遠隔地側でも転送されたデータが常に暗号化されたまま蓄積されるため第三者からの不正アクセスに対してもデータの安全性が確保できるという作用を有する。

【００２４】また、請求項１７に記載の発明は、画像データの記録時に圧縮データから改ざん検出データを生成し、画像データと改ざん検出データを組にして記録部へ記録しておき、再生時は、画像データから新たに生成する改ざん検出データと記録時に生成された改ざん検出データとの比較によって、改ざん検出を行う不正利用防止方法であり、データの不正利用を防止できるという作用を有する。

【００２５】また、請求項１８に記載の発明は、ファイル毎に管理された暗号鍵を保存し、その暗号鍵で暗号化処理を行った画像データを記録し、再生時には入力された暗号鍵で暗号データを復号化することにより、暗号鍵を知らない者による画像の閲覧を防止する不正利用防止方法であり、データの不正利用を防止できるという作用を有する。

【００２６】以下、本発明の実施の形態について、図１から図１２を用いて説明する。

（実施の形態１）図１は本発明の第１の実施の形態における画像記録再生装置の構成を示すブロックである。図１において、１は画像を写すカメラ、２は画像記録再生装置、３は画像を表示するモニタである。画像記録再生装置２を構成する要素は、画像データをデジタル信号で圧縮する画像圧縮部１０、改ざんの有無を検出するデータを生成する改ざん検出データ生成部A11、改ざん検出データ生成部B12、画像データと改ざん検出データをまとめるデータ合成部13、データを記録する記録部14、データ再生時に画像データと改ざん検出データを分離するデータ分離部15、圧縮画像データを伸長する画像伸長部16、改ざんの有無を検出する改ざん検出部17、伸長された画像データのモニタ３への表示を制御する表示制御部18等である。

【００２７】以上のように構成された画像記録再生装置について、図１を用いてその動作を説明する。まず、カメラ３で撮像された電気信号は、画像圧縮部10でアナログ信号からデジタル信号に変換されと共に画像データの情報量を減らすために画像圧縮される。画像圧縮方式としては、JPEG、ウエーブレット変換、DV方式等のフレーム内圧縮方式や、MPEG1 、MPEG4 、H.261 、H.263 等のフレーム間圧縮方式が一般的に利用される。改ざん検出データ生成器A11では、圧縮データに対してチェックサムやＣＲＣ、パリティ等のエラー検出変換を施し、改ざん検出データを生成する。チェックサムでは、全画像データを任意のビット数を１単位として（通常はバイト数の整数倍を用いる）各単位値を加算した合計値あるいは合計値の一部を改ざん検出データとする。ＣＲＣでは、指定した範囲のＣＲＣを計算して改ざん検出データとする。パリティの場合では、画像データ内の各ビットの１の数が偶数か奇数を改ざん検出データとする。

【００２８】データ合成部13では、画像データに付加する付加データの一部に改ざん検出データを埋め込む。一般的に、HDD （ハードディスク）や光ディスクの記録装置では記録する最小単位（セクタ）の容量が決まっており、端数のデータを記録する場合でもセクタ容量の整数倍になるようにデータ量を増やして調整する。また、画像データでは、再生時の条件を埋め込むための付加データ領域を設けた形式が多く、その付加データの一部の未使用領域を利用することもできる。すなわち、多数ある空き領域へ改ざん検出データを埋め込むことが可能である。この場合、画像データの形式は不変であり、従来の装置との互換性が保たれる。

【００２９】図２はこの様子を示している。図２では、画像データ201 を構成する各バイト202 、203 、204 の全てに対して改ざん検出データ生成部A11 でチェックサムを計算し、付加データ205 の一部に改ざん検出データ（チェックサム）206 を埋め込んだ例を示す。なお、付加データ領域は画像データの先頭側、後ろ側のどちらに

配置されてもよい。

【００３０】また、フレーム内圧縮方式の画像データでは、各フレームデータ毎の付加データ内に埋め込むのが好ましい。また、フレーム間圧縮方式の画像データではフレームデータ毎に埋め込むのが好ましいが、関連のある１ブロック（MPEG2 の1GOP単位）のＩピクチャだけでもよい。つまり、フレーム内圧縮では１静止画単位での取り出しが容易であるのに対し、フレーム間圧縮ではブロック先頭のＩピクチャは静止画と同じであるが、後ろのフレームは前後フレームの差分を取るため、差分データを直接改ざんすることは、フレーム内圧縮よりも改ざんが難しいためである。

【００３１】次に、記録部14に記録された画像データを再生する動作について説明する。まず、再生しようとする画像データをフレーム単位で記録部14から読み出す。この時、各フレームには画像データと改ざん検出データがペアで記録されているのでデータ分離部15で改ざん検出データと画像データを分ける。画像データに対しては改ざん検出生成器Ｂ12を用いて改ざん検出データの生成方法と同一方法で再生画像データから改めて改ざん検出データを求める。ここで、改ざん検出データ生成器Ａ11と改ざん検出データ生成器Ｂ12は、分けずに同一のものを使用してもよい。改ざん検出部17では、改ざん検出データ生成部Ｂ12の出力値とデータ分離部15から得られる改ざん検出データを比較する。両者が一致していれば改ざんがなされていないと見なし、もし、両者が不一致の場合には何らかの改ざんが行われていると判断する。

【００３２】改ざん無しの時は、画像伸長部16で伸長された画像データは表示制御部18をそのまま通過し、モニタ3 に映像が映し出される。一方、改ざんが検出された場合には、表示制御部18で、一切の画像の表示を停止してモニタ3 に表示させない。あるいは、画像は表示させるが改ざん発生の警告も重ねて映し出す。

【００３３】以上のように、本発明の実施の形態１によれば、画像データの記録時に圧縮データから改ざん検出データを生成し、画像データと改ざん検出データをペアにして記録部へ記録しておき、再生時は、画像データから新たに生成する改ざん検出データと記録時に生成された改ざん検出データの比較によって、改ざん検出を行うことにより、デジタル画像として記録される画像データの改ざんを検出を、従来の画像データ形式からの変更を少なくして、データ改ざんの有無を簡単にチェックすることができる。

【００３４】なお、フレームデータの全画像データに対して改ざん検出データを生成したが、図３に示すように、画像データの特定の一部分のデータから改ざん検出データを生成してもよい。図３では画像データ201 を構成するデータの一部のブロック217 （201 、202 、203 のバイトで構成）と207 （213 、214 、215 のバイトで構成）からのデータを改ざん検出データ生成部Ａ11へ入力し、改ざん検出データ216 を付加データ205 内に埋め込んだ例を示している。この場合には、全体の計算量を抑えることで、ハード規模や改ざん検出データの生成時間を短くできる利点がある。

【００３５】（実施の形態２）図４は本発明の第２の実施の形態における画像記録再生装置と画像再生装置の構成を示すブロック図である。図４において、カメラ１、モニタ３と符号10～18までは、実施の形態１と同様である。本実施の形態２は、画像記録再生装置２に可換記録媒体21と外部記録装置22を付加したことと、画像再生装置30の間で可換記録媒体21を介して情報交換可能なシステムにしたことである。再生装置30を構成するブロックは、可換記録媒体21を扱える外部記録装置31と、画像データと付加データを分離するデータ分離部32、画像データから改ざん検出データを生成する改ざん検出生成部33、改ざんの有無を検出する改ざん検出部34、圧縮画像の伸長を行う画像伸長部35、改ざんの有無により表示画像を制御する表示制御部36を備えており、画像はモニタ37に表示される。ここでは、可換記録媒体21としてＤＶＤ－ＲＡＭディスクを使用し、外部記録装置22および31としてＤＶＤ－ＲＡＭドライブを使用しているが、他の光ディスクや光磁気ディスク、磁気テープ等の可換記録媒体およびそのドライブを使用してもよい。

【００３６】図４を用いて動作を説明する。まず、画像記録再生装置２で画像データおよび改ざん検出データが記録されるまでの動作は実施の形態１で説明した通りである。記録部14で記録された画像データを外部へ取り出すには、可換記録媒体21へ複製する。複製する場合には、フレームの画像データとその改ざん検出データを対にして行う。例えば、図５に示すように画像ファイルが４つのフレームデータ131 、132 、133 、134 で構成されていた場合に、フレーム（１）～（４）と各フレームに対する付加データ（１）～（４）135 、136 、137 、138 のうちフレーム（１）とフレーム（３）を光ディスク21へ複製する時はフレーム（１）131 、付加データ（１）135 、フレーム（３）133 、付加データ（３）137 を抜き出して可換記録媒体21へ記録する。

【００３７】次に、画像データを記録した可換記録媒体21を画像記録再生装置２以外の再生装置（パソコン等）で再生する場合を説明する。画像再生装置30の外部記録装置31は、可換記録媒体21の再生ができるとする。再生された画像データは、データ分離部32によって付加データ内の改ざん検出データを抜き出す。また、改ざん検出データ生成部33で画像データから改ざん検出データを再度計算する。改ざん検出部34では、両者を比較し、一致する場合は改ざん無し、不一致なら改ざん有りと判断する。改ざん無しの場合には、画像データは画像伸長部35で伸長され、モニタ37に画像が表示される。改ざん有りの場合には、表示制御部36で画像の表示を停止させるか、あるいは警告も重ねて表示させる。以上の動作はソ

フトウエアでも実現できる。

【００３８】以上のように、本実施の形態２によれば、画像記録再生装置２で記録した画像データを画像データと改ざん検出データを組にして光ディスク等の可換記録媒体に複製し、他の外部再生装置でも同様の改ざん検出機構を構築することで、不正が施された可換メディアの再生を簡単に検出することができる。

【００３９】（実施の形態３）図６は本発明の第３の実施の形態における画像再生装置30の構成を示すブロック図である。図６において、可換記録媒体21、30～37は実施の形態２における画像再生装置30と同一の機能を有する。実施の形態２との違いは、電子透かし処理部38と、可換メディア39への記録が可能である点である。

【００４０】図６を用いて動作を説明する。可換記録媒体21から画像データが再生され、改ざん検出が行われるまでの動作は実施の形態２で説明した動作と同じである。記録画像の利用目的によっては、簡便にパソコンの汎用ソフトで扱えるデータ形式で取り出せる機能が便利なこともある。この場合にも改ざん等の不正利用の防止策を講ずる必要がある。

【００４１】そこで、改ざんされていない画像データが再生され、この画像データを更に静止画として外部へ取り出す場合に、電子透かし処理部38で画像に電子透かしを埋め込んでから可換メディア39（光ディスク、光磁気ディスク、フロッピーディスク等）へ記録するようにする。電子透かしで埋め込むデータは、画像が記録され日時、時間、画像を撮影した装置、人物を特定できる識別子（IDデータ）等である。

【００４２】すなわち、可換記録媒体21と同様に画像データに改ざん検出データを添付し続ける複製の場合、再生時に改ざん検出機能を有する再生装置が必須になるため、少ない画像データを汎用ソフトで利用する場合には向かない。そこで、画像データそのものに電子透かしで管理用の情報を埋め込む方法が優れている。もし、汎用ソフトでの改ざん等が行われた場合には、画像に埋め込まれた透かしデータの一部が破壊されるため、この破壊を検出できるソフトによって改ざんの有無を検出できる。また、原画に関する情報も画像と共に継承され、何処ででも記録条件等のデータを画像から引き出せる。

【００４３】以上のように、本実施の形態３によれば、画像再生装置30で画像をさらに別メディアへ複製する際に、電子透かしを埋め込む電子透かし処理部38を介して行うことで、複製後のデータの改ざん検出および画像の識別をが容易に行うことができる。

【００４４】（実施の形態４）図７は本発明の第４の実施の形態における画像記録再生装置と画像再生装置の構成を示すブロック図である。図７において、カメラ１、モニタ３と符号10～18までは、実施の形態１と同様である。また、符号32から39までは実施の形態３と同様な動作をする。本実施の形態４は、画像記録再生装置２に暗号化部40、暗号鍵管理部41、ネットワークインタフェース部42を設けるとともに、画像再生装置30にネットワークインターフェース43と、復号化部44、暗号鍵管理部45を設けたものである。

【００４５】図７を用いて動作を説明する。画像記録再生装置２において、カメラ1 の画像データが改ざん検出データと共に記録部14へ記録されるまでの過程は実施の形態１で述べた通りである。記録部14に記録されたデータを画像再生装置30へ伝送するために、まず画像記録再生装置30の暗号鍵管理部45では画像データ暗号用の共通鍵（Ａ）を送る際に使用する公開鍵（Ｂ）を画像記録再生装置２へ伝送する。次に、画像記録再生装置2 では、暗号鍵管理部41において受信した公開鍵（Ｂ）を使って画像暗号化用の共通鍵（Ａ）を暗号化し、共通鍵（Ａ’）として画像再生装置30へ送る。画像記録再生装置30では、自分が送信した公開鍵（Ｂ）と対の秘密鍵（Ｃ）を利用して暗号化されて送られてきたきた共通鍵（Ａ’）を復号化して共通鍵（Ａ）を求め、暗号鍵管理部45で管理する。以上で共通鍵（Ａ）の交換が完了する。この共通鍵の交換では、画像記録再生装置2 側の暗号鍵管理部41と画像再生装置30側の暗号鍵管理部45が同じ鍵管理テーブルを持ち、テーブル番号の交換で暗号鍵を一致させる方法でも構わない。

【００４６】次に、画像データを送信する際は、記録部14内の画像データとそれに関連する付加データを必ず１組で送信する。画像記録再生装置2 では、暗号鍵管理部41内の共通鍵（Ａ）を用いて暗号化部40で画像データと付加データをまとめて暗号化する。この暗号化データはネットワークインターフェース42を通して画像再生装置30へ伝送される。伝送方法には、ISDNや一般電話回線を利用した通信方法や、インターネット網を利用した通信方法、限られたエリア内で構築されたLAN （Local Area Network）等、通信方法は問わない。

【００４７】画像再生装置30では、伝送されてきたデータをネットワークインターフェース43で受信し、暗号鍵管理部45が管理する共通鍵（Ａ）で受信したデータを復号化部44で復号化して記録部46へ記録する。すなわち、記録部14から記録部46へデータが複製される。記録部46に記録されたデータに対して、再生時にデータ分割部32、改ざん検出部データ生成部33、改ざん検出部34を用いて画像データの改ざん検出を行って、改ざんデータに対しては非表示あるいは警告表示を行う動作は実施の形態３と同じである。また、さらに可換メディア39へ小数のデータを複製する場合には、電子透かし処理部38にて画像データそのものに電子データを埋め込む。この方法は実施の形態３で述べたと同じである。

【００４８】以上のように、本実施の形態４によれば、画像記録再生装置２と画像再生装置30の間での画像データおよび付加データの交換の際に、暗号鍵管理部41、54、ネットワークインターフェース42、43と暗号化部4

0、復号化部44を用いて、データを暗号して送ることにより、通信中に第三者がデータを盗み、内容を確認することを防止することができる。

【００４９】（実施の形態５）図８は本発明の第５の実施の形態における画像記録再生装置の構成を示すブロック図である。図８において、１はカメラ、３はモニタ、50は画像記録再生装置である。画像記録再生装置50を構成する要素は、画像圧縮部10、画像を記録・保存・再生できる記録部14、圧縮画像を伸長する画像伸長部16、伸長された画像データのモニタ３への表示を制御する表示制御部18、データの暗号化を行う暗号化処理部51、暗号鍵を管理する暗号鍵記録部52、暗号鍵を入力する鍵入力部53、暗号データを復号する復号化処理部54である。カメラ１、モニタ３、画像圧縮部10、記録部14、画像伸長部16、表示制御部18は図１と同様のものである。

【００５０】図８を用いて動作を説明する。まず、鍵入力部53を通してデータ暗号化用の暗号鍵（Ａ）を入力し、暗号鍵（Ａ）を暗号鍵記録部52に記録しておく。カメラ1で撮像された画像信号は、画像圧縮部10でデジタルの画像データに変換された後、情報量を減らすための画像圧縮処理が施される。画像圧縮部10で圧縮された画像データは、暗号鍵記録部52に記録された暗号鍵（Ａ）を用いて暗号化処理部51で暗号化される。この時、処理されるデータ量が多いため、暗号化速度の早い共通鍵暗号方式を用いる方法が良いが、公開鍵暗号でも構わない。また、暗号化としては、ある規則に則ったデータスクランブルや、データに特定値の四則演算を施した方式も含めることができる。つまり、圧縮データそのものに何らかの処理を施し、そのままでは利用できない処理を意味する。また、暗号化する単位は１フレーム単位で行うことが望ましい。理由は、再生する際に必要な部分の復号だけで済むためである。

【００５１】暗号化された暗号化データは、記録部14に記録される。この時、図９のように記録した画像データのファイル番号と、暗号化した時の暗号鍵は暗号鍵記録部52において関連づけて管理しておく。例えば、KeyAとファイル（１）、KeyBとファイル（２）のようにする。暗号鍵記録部52には、EEPROM等の書換可能な不揮発性メモリを用いることが望ましい。理由は、電源を落としても消えないようにすることと、記録部14以外に保存することで記録部14が取り外されても外部で再生することができないようすることである。

【００５２】再生時は、記録部14から暗号化データを再生し復号化処理部54へデータを入力する。復号化処理部54では、新たに鍵入力部53から入力された鍵（Ｄ）で復号処理を行う。この時、入力された鍵（Ｄ）と暗号化した鍵（Ａ）が一致すれば正しい圧縮データが得られ、画像伸長部16を通して映像がモニタ３に表示される。しかし、入力された暗号鍵（Ｄ）が画像暗号鍵（Ａ）と一致していなければ、復号化されたデータは画像伸長部16で伸長しても正しい映像にはならない。つまり、本装置で画像データを再生するには正しい暗号鍵を知っている場合しか映像を見ることができないようになる。

【００５３】一方、再生時に、鍵入力部53から再入力される鍵（Ｄ）を利用せずに常に再生できるようにするためには、暗号鍵記録部52に記録されている暗号鍵（Ａ）によって復号処理部54を動作させることで、正しく復号化された映像を見ることができる。つまり、再生ファイル毎に関連づけて暗号鍵が管理されているので、暗号に用いた暗号鍵を参照すればよい。

【００５４】以上のように、本実施の形態５によれば、暗号鍵記録部52にファイル毎に管理された暗号鍵を保存し、その暗号鍵で暗号化処理を行った画像データを記録部14へ保存し、再生時には鍵入力部53で入力される暗号鍵で暗号データを復号化処理部54で復号化することにより、暗号鍵を知らない人物による画像の閲覧を防止することができる。

【００５５】（実施の形態６）図10は本発明の実施の形態６における画像記録再生装置と画像再生装置の構成を示すブロック図である。図10において、符号１、３、10、14、16、18、51～54は実施の形態５で説明した要素と同じである。55は暗号鍵を暗号化する暗号鍵暗号部、56はデータ合成部、57は外部記録装置、58は可換記録媒体で、以上で画像記録再生装置50が構成される。一方、画像再生装置60は、可換記録媒体58と、外部記録装置62、データ分離部63、暗号鍵復号部64、鍵入力部65、選択部66、復号化処理部67、画像伸長部68、表示制御部69、電子透かし処理部38で構成される。鍵入力部65と復号化処理部67と画像伸長部68は、画像記録再生装置50の鍵入力部53と復号化処理部54と画像伸長部16と同じものである。また、37は画像再生装置60用のモニタで、39は画像切り出し記録するための可換メディアである。

【００５６】図10を用いて動作を説明する。カメラ１で撮像された信号が画像圧縮部10、暗号化処理部51を通して圧縮・暗号化され、記録部14に記録されるまでの過程は実施の形態５で説明した動作と同じであるので、ここでは記録部14に記録されたデータを外部記録装置57を通して可換記録媒体58（光ディスク、光磁気ディスク、フロッピーディスク、リムーバブルハードディスク等）に記録する動作を説明する。図11は、暗号鍵記録部52内と記録部14内に記録されているデータの模式図である。記録部14には画像ファイル（暗号化データ）としてファイル（１）、（２）、（３）が記録されており、暗号鍵記録部52には、ファイル（１）、（２）、（３）に対する暗号鍵として、それぞれ鍵Key Ａ、鍵Key Ｂ、鍵Key Ｃとしている。

【００５７】ファイル（２）を可換記録媒体58へ記録する場合を例にとると、記録部14からファイル（２）を再生し、データ合成部56へ渡す。一方、暗号鍵記録部52から鍵Ｂを取り出し暗号鍵暗号部55で暗号化し、鍵Key

B'を生成してデータ合成部56へ渡す。暗号鍵を生成する際の暗号鍵は装置が持っている独自の鍵を利用するものとする。データ合成部56では、ファイル（２）と鍵Key B'を一組として外部記録装置57を通して可換記録媒体58へ記録する。なお、この時、ファイル（２）と鍵B'は、可換記録媒体58の連続する位置に記録する必要はなく、ペアであることを管理して記録することを意味する。

【００５８】画像再生装置60では、画像記録再生装置50で記録された可換記録媒体58を外部記録装置62で再生する。次に、データ分離部63で、ファイル（２）と対応する鍵Key B'を分ける。また、鍵入力部65では、再生する人物が鍵を入力する。ファイル（２）は復号化処理部76へ入力され、同時に鍵入力部での入力鍵で復号を行う。もし、暗号時の鍵と入力鍵が同じならば、正しい映像が画像伸長部68および表示制御部69を通じてモニタ37に表示される。もし、両者が不一致ならば、正しいデータが再生されない。

【００５９】なお、画像再生装置60で、鍵入力無しで画像の再生を行うために、暗号鍵復号部64を設け、データ分離部63から得られる鍵B'を復号化し、鍵Bを得る。この鍵Bを用いて復号化処理部67で画像データを復号化する。鍵B'を復号化する暗号鍵は、暗号鍵暗号部55と同一の装置独自の暗号鍵を用いる。この時、記録されている鍵を利用するかどうかは選択部54で決まる。また、復号化された画像データの一部をさらに他の可換メディア39に複写する場合には、実施の形態３で説明したように、電子透かし処理部38で画像の記録時間、記録装置等のデータを電子透かしとして埋め込む機能も備えることもできる。

【００６０】以上のように、本実施の形態６によれば、画像記録再生装置50では、暗号化された画像を複写する際に画像データの暗号化使用した暗号鍵を暗号化して可換記録媒体58に一緒に記録する。また画像再生装置60で可換記録媒体58を再生する際には、可換記録媒体58から画像データと暗号鍵データを分離し、画像データの復号化には新たに入力した暗号鍵、あるいは可換記録媒体58に記録されている暗号化された暗号鍵を復号化した暗号鍵を用いるようにする。画像再生装置60とは別の装置で画像を再生する際にも、暗号化された画像データの再生を第三者が勝手に行えないようにすることもでき、かつ、アプリケーションによっては自由に再生を行うことも可能となる。

【００６１】（実施の形態７）図12に本発明の実施の形態７における画像記録再生装置と画像再生装置の構成を示すブロック図である。図12において、カメラ１、モニタ３は前述の通りである。また、画像記録再生装置70は、実施の形態６と同様の動作をする10、14、16、18、37、39、51、52、53、54の他に、以下のブロックを新たに備えている。71は暗号鍵を暗号化する暗号鍵暗号部、72はネットワークと接続するネットワークインターフェースである。73は電話回線やLAN 等の一般的なネットワーク網である。また、画像再生装置80は、画像記録装置70とネットワーク73を介して接続可能とし、以下の新しいブロックで構成される。74はネットワークインターフェース、75は暗号鍵管理部、76は記録部で、その他は実施の形態６と同様の動作をする鍵入力部65、復号化処理部67、画像伸長部68、表示制御部69、電子透かし処理部38である。

【００６２】以上のように構成された画像記録再生装置および画像再生装置の動作を説明する。カメラ１で撮像された電気信号が圧縮・暗号化され記録部14に保存されるまでの動作は実施の形態６と同じである。ここで、記録部14の画像データをネットワーク73を通じて遠隔地にある画像再生装置80で再生する場合を考える。ネットワーク73上に画像データを送信する場合には、既に述べたように画像の盗み見に対する対策が必要となる。そこで、本実施の形態では、既に暗号化された画像データであるため、そのまま送信してもデータの安全が確保される。あとは暗号鍵を安全に送ればよい。そこで、画像再生装置80側の暗号鍵管理部75で公開鍵暗号方式に則った公開鍵（Ｅ）を生成し、ネットワークインターフェース74を通して画像記録再生装置70側へ送る。画像記録再生装置70では、ネットワークインターフェース72を介して公開鍵（Ｅ）を受信し、暗号鍵暗号部71へ送る。ここで画像の再生要求が画像再生装置80から発せられた時には、指定された再生ファイルに対する暗号鍵（Ｆ）を暗号鍵暗号部71で受信した公開鍵（Ｅ）で暗号化（Ｆ'）し、ネットワーク73を介して画像再生装置80の暗号鍵管理部75へ送り返す。暗号鍵管理部75では、送られてきた暗号鍵（Ｆ'）を復号して暗号鍵（Ｆ）を入手する。指定された画像データは、そのままネットワーク73を利用して記録部76へ伝送される。

【００６３】次に記録部76に複写された画像データは、鍵入力部65から入力された暗号鍵（Ｇ）を用いて復号化処理部67で復号化される。この時、入力した暗号鍵（Ｇ）が暗号鍵（Ｆ）と間違っていれば正しい映像は再生されない。正しい暗号鍵が入力された時は、画像伸長部68で伸長された画像データが表示制御部69を介してモニタ37に表示される。この暗号鍵を入力する方法で、第三者からの無断の画像再生を防止することができる。一方、暗号鍵入力をせずに、そのまま再生しても良い画像に対しては、暗号鍵管理部75が管理している暗号鍵（Ｆ）を用いて復号化処理部76を動作させることで、常に正しく復号化される。そして、画像伸長部68での伸長により表示制御部69を介してモニタ37に映像が表示される。さらに、可換メディア39に一部を複製する場合には、実施の形態６と同様に電子透かし処理部38で必要なデータを画像に埋め込むことができる。

【００６４】以上のように、本実施の形態７によれば、

画像記録再生装置70側で記録部14に暗号化して記録されている画像データをネットワーク73経由で送信する際に、画像データを暗号化した暗号鍵を暗号化して送信する暗号鍵暗号部71を設け、受信側の画像再生装置80では、画像データは暗号化されたまま記録部76に記録され、再生時に暗号鍵の管理を暗号鍵管理部75で管理しながら、必要な画像のみを複合化処理部67で復号化して再生することで、無断での画像再生を完全に防止するシステムを構築することができる。

【００６５】

【発明の効果】以上のように本発明は、画像データの記録時に圧縮データから改ざん検出データを生成し、画像データと改ざん検出データを組にして記録部へ記録しておき、再生時は、画像データから新たに生成する改ざん検出データと記録時に生成された改ざん検出データとの比較によって、改ざん検出を行うようにしたものであり、また、ファイル毎に管理された暗号鍵を保存し、その暗号鍵で暗号化処理を行った画像データを記録し、再生時には入力された暗号鍵で暗号データを復号化することにより、暗号鍵を知らない者による画像の閲覧を防止するようにしたものであり、デジタルで記録される画像データを記録再生する装置およびシステムにおいて、第三者による改ざんを防止し、デジタル画像の信憑性を高めることができるという効果が得られる。

【図面の簡単な説明】

【図１】本発明の実施の形態１における画像記録再生装置のブロック図

【図２】本発明の実施の形態１におけるデータ計算方法の動作説明図

【図３】本発明の実施の形態１における別のデータ計算方法の動作説明図

【図４】本発明の実施の形態２における画像記録再生装置および画像再生装置のブロック図

【図５】本発明の実施の形態２における画像データ複写の動作説明図

【図６】本発明の実施の形態３における画像再生装置のブロック図

【図７】本発明の実施の形態４における画像記録再生装置および画像再生装置のブロック図

【図８】本発明の実施の形態５における画像記録再生装置のブロック図

【図９】本発明の実施の形態５における画像記録再生装置内のデータ配置例の模式図

【図１０】本発明の実施の形態６における画像記録再生装置および画像再生装置のブロック図

【図１１】本発明の実施の形態６における画像データ複写の動作説明図

【図１２】本発明の実施の形態７における画像記録再生装置および画像再生装置のブロック図

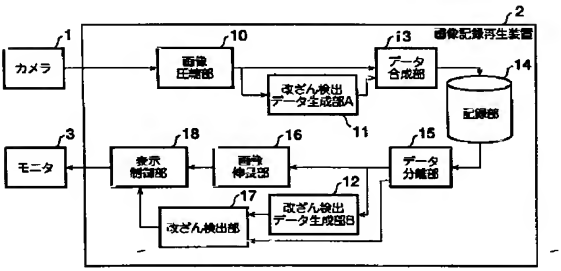
【図１３】従来例の画像記録再生装置のブロック図

【符号の説明】

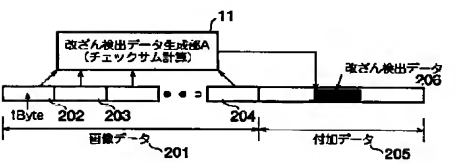
1　カメラ
2　画像記録再生装置
3　モニタ
10　画像圧縮部
11　改ざん検出データ生成部Ａ
12　改ざん検出データ生成部Ｂ
13　データ合成部
14　記録部
15　データ分離部
16　画像伸長部
17　改ざん検出部
18　表示制御部
21、58、61　可換記録媒体
22、31、57、62　外部記録装置
30　画像再生装置
32　データ分離部
33　改ざん検出データ生成部
34　改ざん検出部
35　画像伸長部
36　表示制御部
37　モニタ
38　電子透かし処理部
39　可換メディア
40　暗号化部
41　暗号鍵管理部
42、43、72、74　ネットワークインターフェース
44　復号化部
45　暗号鍵生成部
46、76　記録部
50　画像記録再生装置
51　暗号化処理部
52　暗号鍵記録部
53　鍵入力部
54　復号化処理部
55　暗号鍵暗号部
56　データ合成部
60　画像再生装置
63　データ分離部
64　暗号鍵復号部
65　鍵入力部
66　選択部
67　復号化処理部
68　画像伸長部
69　表示制御部
70　画像再生装置
71　暗号鍵暗号部
75　暗号鍵管理部
101　カメラ
102　画像記録再生装置

103　モニタ
104　A/D 変換器
105　画像圧縮エンコーダ
106　記録部
107　画像伸長デコーダ
108　D/A 変換器
131 ～134　フレームデータ
135 ～138　付加データ
201　画像データ
202 ～204 、210 ～215　画像データの１バイト
205　付加データ
206 、216　改ざん検出データ
217 、218　計算対象ブロック

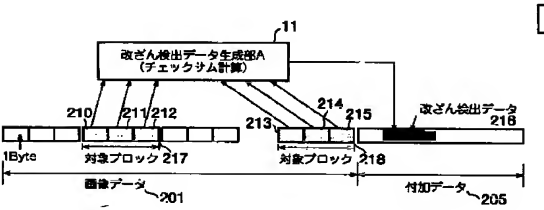
【図１】



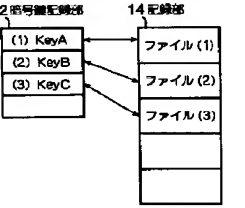
【図２】



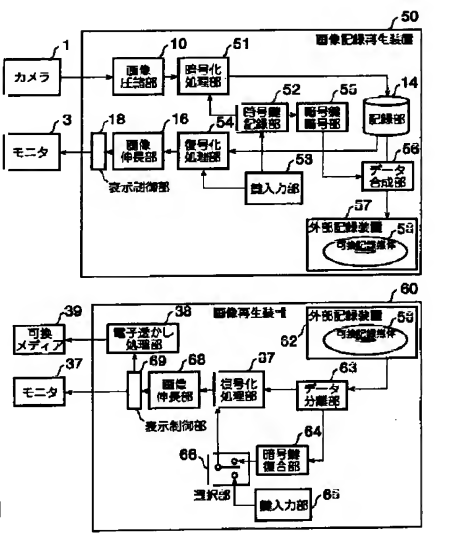
【図３】



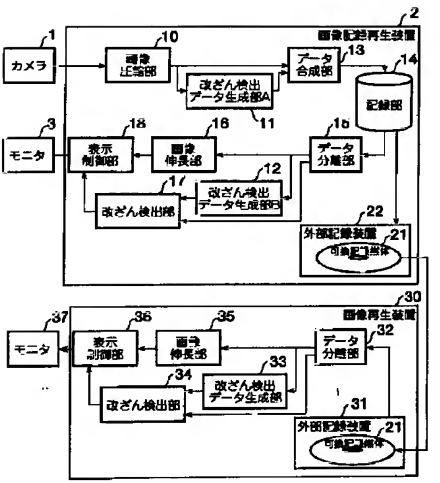
【図９】



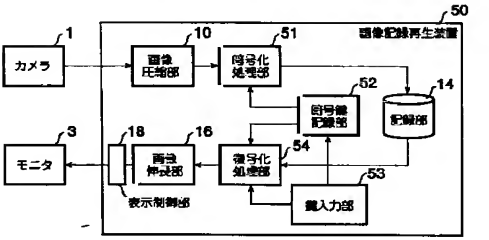
【図１０】



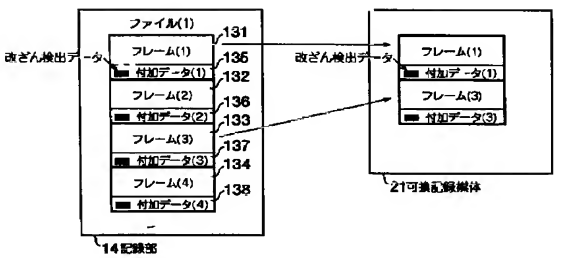
【図4】


画像記録再生装置
カメラ
画像圧縮部
データ合成部
改ざん検出データ生成部A
記録部
モニタ
表示制御部
画像伸長部
データ分離部
改ざん検出データ生成部B
改ざん検出部
外部記録装置
可換記録媒体
画像再生装置
モニタ
表示制御部
画像伸長部
データ分離部
改ざん検出データ生成部
改ざん検出部
外部記録装置
可換記録媒体

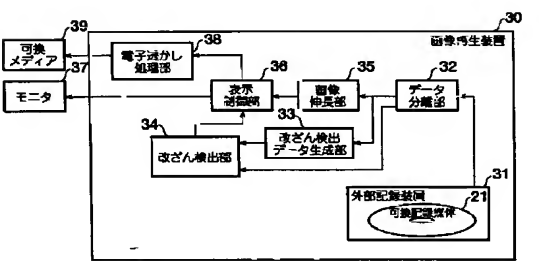
【図8】


画像記録再生装置
カメラ
画像圧縮部
暗号化処理部
暗号鍵記録部
記録部
モニタ
画像伸長部
復号化処理部
表示制御部
鍵入力部

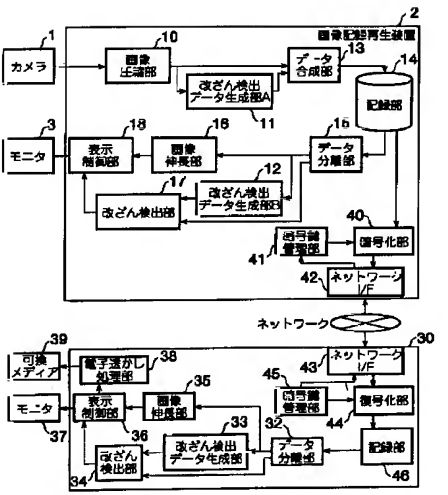
【図5】


改ざん検出データ
ファイル(1)
フレーム(1)
付加データ(1)
フレーム(2)
付加データ(2)
フレーム(3)
付加データ(3)
フレーム(4)
付加データ(4)
14記録部
改ざん検出データ
フレーム(1)
付加データ(1)
フレーム(3)
付加データ(3)
21可換記録媒体

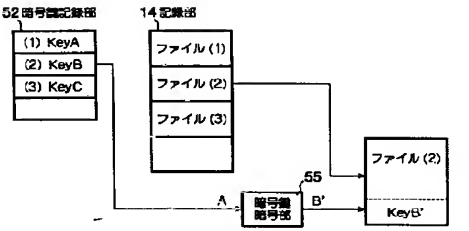
【図6】


可換メディア
電子透かし処理部
画像再生装置
モニタ
表示制御部
画像伸長部
データ分離部
改ざん検出データ生成部
改ざん検出部
外部記録装置
可換記録媒体

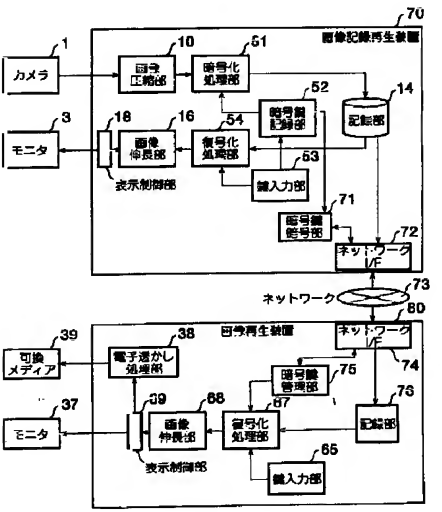
【図7】


画像記録再生装置
カメラ
画像圧縮部
データ合成部
改ざん検出データ生成部A
記録部
モニタ
表示制御部
画像伸長部
データ分離部
改ざん検出データ生成部B
改ざん検出部
暗号鍵管理部
暗号化部
ネットワークI/F
ネットワーク
可換メディア
電子透かし処理部
画像処理部
復号化部
改ざん検出データ生成部
データ分離部
記録部
改ざん検出部

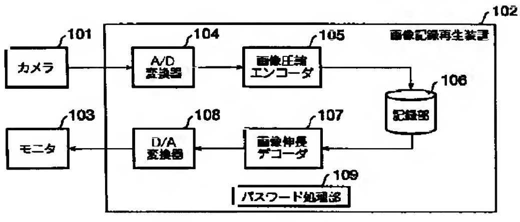
【図11】


52 暗号鍵記録部
(1) KeyA
(2) KeyB
(3) KeyC
14 記録部
ファイル(1)
ファイル(2)
ファイル(3)
A
暗号鍵暗号部
B'
ファイル(2)
KeyB'

【図12】


画像記録再生装置
カメラ
画像圧縮部
暗号化処理部
暗号鍵記録部
記録部
モニタ
表示制御部
画像伸長部
復号化処理部
鍵入力部
暗号鍵暗号部
ネットワークI/F
ネットワーク
画像再生装置
可換メディア
電子透かし処理部
暗号鍵管理部
画像伸長部
復号化処理部
記録部
鍵入力部

【図13】



フロントページの続き

(51)Int.Cl.7		識別記号	FI			(参考)
H04N	1/41		H04N	1/41	Z	
	5/765			5/781	510F	
	5/781					

Fターム(参考) 5B017 AA06 BA05 BA07 BB03 CA07 CA08 CA09 CA16
5C053 FA13 FA15 FA23 GA11 GB06 GB36 GB37 HA29 JA21 KA21 KA24 KA25 LA01 LA06 LA14
5C078 CA00 DA00 DA01 DA02
5J104 AA08 AA14 LA05 NA27
9A001 BB01 BB03 BB04 CC04 CC07 CC08 EE03 EE04 EE05 FF03 HH27 HH28 JJ25 KK37 LL02 LL03